From: Aaron Williams
To: Microsoft ATR
Date: 12/9/01 4:56pm
Subject: Microsoft settlement

Hi,

After looking at the settlement, I think it may make things worse than they already are. For example, right now there is a popular piece of software called Samba (see http://www.samba.org/). Samba allows non-Microsoft operating systems such as Linux, Solaris, and many others to interoperate with Windows. Samba is used by many corporations and even the US government. Your settlement would effectively kill Samba. You see, Samba is not written by a corporation, but is a not for profit project. Samba relies on Microsoft's encryption and authentication protocols for interoperability. By allowing Microsoft to keep this proprietary effectively kills Samba.

There is absolutely no reason for Microsoft to keep security protocols undocumented. Security through obscurity has been proven time and again to be a failure. DeCSS is a perfect example. The DVD industry tried to keep their method of encrypting DVDs a trade secret. It was only a matter of time until someone reverse engineered it. Not only that, but once it was reverse engineered and analyzed it was found to be extremely weak encryption. It was supposed to be 40 bits, which while not strong, is time consuming to crack. It was found that only 16 bits needed to be found, or 65,536 combinations. It only takes a modern computer a few milliseconds to crack the DVD encryption, even without the keys.

Another example is Microsoft's media authentication code for making multimedia files that cannot be copied. It has been reverse engineered and well documented how to defeat, even though it was proprietary and Microsoft tried to make it difficult.

Microsoft should be forced to fully document every protocol (method of exchanging information over a network) and all of their file formats.

For example, nobody can effectively compete with Microsoft Office because the file formats are proprietary and not documented. Most of the current support for alternative office products (like Star Office) that can read Microsoft documents do so by trying to reverse-engineer Microsoft's files. This is very difficult to do and results in less-than-perfect reading of Microsoft documents in non-Microsoft products.

And finally, Microsoft currently has a licensing restriction on PC manufacturers such that they cannot install any software that modifies the boot process. This requirement prevents manufacturers from installing Linux and Windows on the same computer. When Linux, or any

other operating system, is installed on the same computer as Windows, a boot selector must be installed. Microsoft's restriction significantly hampers PC manufacturers who can install either Windows or Linux (or any other operating system) but not both.

I propose the following must be part of the settlement:

1. Microsoft must fully document all protocols (including security related protocols).
2. Microsoft must fully document the format of any file that is used for saving or exchanging information.
3. Microsoft may not restrict other operating systems being installed on computers at the same time as Windows, even if the boot operation is modified.

The documentation must also be available to everyone, not just licensed coporations. This will help level the playing field and can in fact help grow the economy since there will be more products to choose from and new features can be added by 3rd parties that otherwise could not.

-Aaron Williams